PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-116538
(43)Date of publication of application : 02.05.1997

(51)Int.Cl. H04L 12/24
H04L 12/26
H04L 12/28

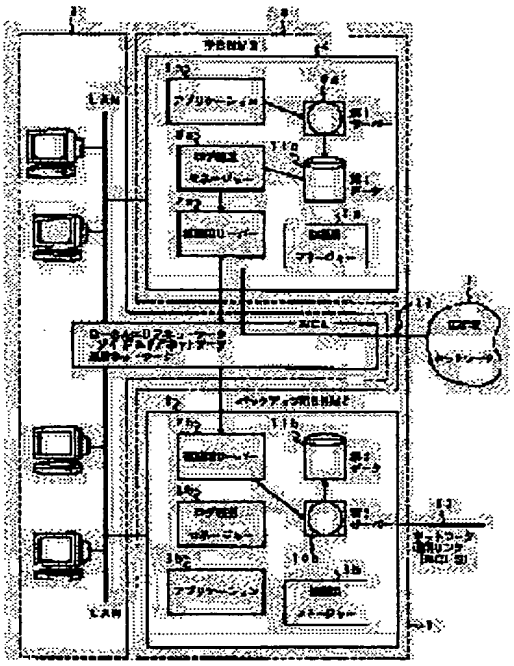
(21)Application number : 08-156811
(22)Date of filing : 18.06.1996

(71)Applicant : NEC CORP
(72)Inventor : AJITSUTO JII HEMADEII

(30)Priority
Priority number : 95 491828 Priority date : 19.06.1995 Priority country : US

(54) FAULT-TOLERANT WIDE BAND NETWORK MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the management system which contains a main backup structure to automatically restore a crushing fault if occurred.
SOLUTION: A backup BNMS data base maintains the synchronism with a main BNMS data base via a duplication data server. If the main BNMS has such a trouble that causes a communication fault against a wide band network, an NCL is automatically switched to the backup BNMS from the main BNMS. Thus the backup BNMS monitors and controls a BNM in place of the main BNMS. That is, the backup BNMS takes over the management of the network and functions as the main BNMS. When the fault of the main BNMS is recovered, the main BNMS takes over the function of the backup BNMS that so far functioned as the main BNMS.



LEGAL STATUS

[Date of request for examination]	18.06.1996
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2998789
[Date of registration]	05.11.1999
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－116538

(43)公開日　平成９年(1997)５月２日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/24		9466－5K	Ｈ０４Ｌ	11/08	
	12/26		9466－5K		11/20	Ｄ
	12/28		9466－5K			Ｃ

審査請求　有　　請求項の数23　ＯＬ　外国語出願　（全 40 頁）

(21)出願番号　特願平8－156811

(22)出願日　平成８年(1996)６月18日

(31)優先権主張番号　０８／４９１８２８

(32)優先日　1995年６月19日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　アジット　ジー．ヘマディー
アメリカ合衆国，75024　テキサス，プラノ，ウインステッド　ドライヴ　6113

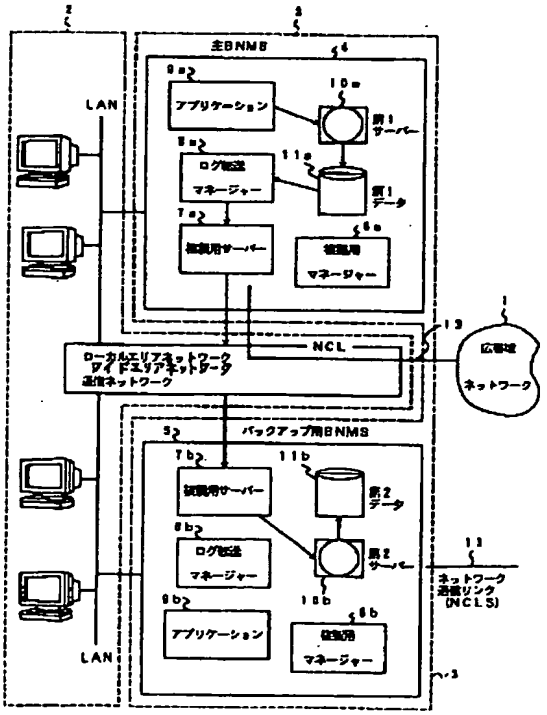
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　フォールトトレラント広帯域ネットワーク管理システム

(57)【要約】　（修正有）

【課題】　壊滅的な障害の発生の際に自動復旧を行うため主・バックアップ構造を備えた管理システムを提供する。

【解決手段】　バックアップ用ＢＮＭＳのデータベースは、各ＢＮＭＳの複製用データサーバーを介して、主ＢＮＭＳのものとの同期を維持する。主ＢＮＭＳと広帯域ネットワークＢＮ１との間の通信障害を引き起こすような故障が、主ＢＮＭＳに発生すると、主ＢＮＭＳからバックアップ用ＢＮＭＳへ自動的にＮＣＬを切り替えて、バックアップ用ＢＮＭＳがＢＮを監視し制御する動作を引き継ぐ。バックアップ用ＢＮＭＳがネットワークの管理を引き継ぐと、主ＢＮＭＳの役割を果たすことになる。本来の主ＢＮＭＳが再び動作可能になった時には、本来のバックアップ用ＢＮＭＳが主ＢＮＭＳの役割を果たしているので、バックアップ用ＢＮＭＳの役割を引き継ぐ。



1

【特許請求の範囲】

【請求項１】　少なくとも一つのネットワーク構成要素から成る広帯域ネットワークを、第１のネットワーク通信リンクを介して管理するための主（プライマリ）広帯域ネットワーク管理システムを備えるとともに、前記主広帯域ネットワーク管理システムと連係するバックアップ用広帯域ネットワーク管理システムを備えた広帯域ネットワーク管理システムにおいて、前記主管理システムにおける故障状態に応答して自動復旧を行うための方法であって、前記方法は、前記主広帯域ネットワーク管理システムにおける故障状態に応答して、前記バックアップ用広帯域ネットワーク管理システムと、前記広帯域ネットワーク内の前記少なくとも一つのネットワーク構成要素との間に第２のネットワーク通信リンクを形成するステップと、前記第２のネットワーク通信リンクを介して、前記広帯域ネットワークを管理する役割を行うように前記バックアップ用広帯域ネットワーク管理システムを作動させるステップとを有することを特徴とする方法。

【請求項２】　前記広帯域ネットワーク管理システムの起動の前に、前記主ネットワーク管理システムに設けられた第１のテーブルに、少なくとも一つのインターネットプロトコルアドレスをあらかじめ記憶させるステップと、前記バックアップ用ネットワーク管理システムに設けられた第２のテーブルに、少なくとも一つのインターネットプロトコルアドレスをあらかじめ記憶させるステップとをさらに有することを特徴とする請求項１に記載の自動復旧方法。

【請求項３】　前記第１のネットワーク通信リンクが、前記主ネットワーク管理システムの前記第１のテーブルに記憶された前記少なくとも一つのインターネットプロトコルアドレスによって規定され、前記第２のネットワーク通信リンクが、前記バックアップ用広帯域ネットワーク管理システムの前記テーブルに記憶された前記少なくとも一つのインターネットプロトコルアドレスを用いて形成されることを特徴とする請求項２に記載の自動復旧方法。

【請求項４】　前記バックアップ用広帯域ネットワーク管理システム作動時には、前記バックアップ用広帯域ネットワーク管理システムが、本来の主広帯域ネットワーク管理システムの役割を引き継ぐことを特徴とする請求項１に記載の自動復旧方法。

【請求項５】　前記本来の主広帯域ネットワーク管理システムの修復時には、前記本来の主広帯域ネットワーク管理システムが、前記バックアップ用広帯域ネットワーク管理システムの役割を引き継ぐことを特徴とする請求項４に記載の自動復旧方法。

【請求項６】　前記主広帯域ネットワーク管理システムと前記バックアップ用広帯域ネットワーク管理システムの両方に存在するマネージャーおよびエージェントオブジェクトに基づいたフォールトトレラントメカニズムを用いて、前記主広帯域ネットワーク管理システムと前記バックアップ用広帯域ネットワーク管理システムの両方を故障について監視するステップをさらに有することを特徴とする請求項１に記載の自動復旧方法。

2

【請求項７】　前記主広帯域ネットワーク管理システムにおける前記マネージャーオブジェクトと、前記バックアップ用広帯域ネットワーク管理システムにおける前記エージェントオブジェクトとの間で、周期的な心拍メッセージを送るステップをさらに有することを特徴とする請求項６に記載の自動復旧方法。

【請求項８】　前記バックアップ用広帯域ネットワーク管理システムにおける前記エージェントオブジェクトが周期的なベースでの心拍を受け損なった場合に、前記主広帯域ネットワーク管理システムにおける故障状態を検出するステップをさらに有することを特徴とする請求項７に記載の自動復旧方法。

【請求項９】　前記主広帯域ネットワーク管理システムと前記バックアップ用広帯域ネットワーク管理システムの各々において、前記マネージャーオブジェクトと前記エージェントオブジェクトのうちの一方のみが、任意の時点において活性化されていることを特徴とする請求項６に記載の自動復旧方法。

【請求項１０】　前記主広帯域ネットワーク管理システムにおける故障状態の検出後、前記主広帯域ネットワーク管理システム内の前記エージェントオブジェクトを活性化させるステップと、前記主広帯域ネットワーク管理システム内の前記マネージャーオブジェクトを非活性化させるステップと、前記バックアップ用広帯域ネットワーク管理システム内の前記マネージャーオブジェクトを活性化させるステップと、前記バックアップ用広帯域ネットワーク管理システム内の前記エージェントオブジェクトを非活性化させるステップと、前記バックアップ用広帯域ネットワーク管理システムと前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間に、コムサーバー（ｃｏｍｍｓｅｒｖｅｒ）オブジェクトを用いて前記第２のネットワーク通信リンクの形成を開始するステップとをさらに有し、正常な動作状態の下では、前記主広帯域ネットワーク管理システムの前記マネージャーオブジェクトと、前記バックアップ用広帯域ネットワーク管理システムの前記エージェントオブジェクトとが活性化されていることを特徴とする請求項８に記載の自動復旧方法。

【請求項１１】　前記バックアップ用広帯域ネットワーク管理システムと前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間に、前記第２のネットワーク通信リンクを形成した後、前記バックアップ用広帯域ネットワーク管理システムと、前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間の、前記少なくとも一つのネット

ワーク通信リンクを活性化させ、これにより、前記主広帯域ネットワーク管理システムから前記バックアップ用広帯域ネットワーク管理システムへ、前記広帯域ネットワークを管理する役割を切り替えるステップをさらに有することを特徴とする請求項１０に記載の自動復旧方法。

【請求項１２】　前記本来の主広帯域ネットワーク管理システムが修復された後、前記本来の主広帯域ネットワーク管理システムは前記バックアップ用広帯域ネットワーク管理システムの役割を引き継ぐことを特徴とする請求項１１に記載の自動復旧方法。

【請求項１３】　前記心拍メッセージは複数個の冗長性（ｒｅｄｕｎｄａｎｔ）物理リンクを経て送られることを特徴とする請求項７に記載の自動復旧方法。

【請求項１４】　前記バックアップ用広帯域ネットワーク管理システムにおいて故障が検出された時、アラームを発生するステップをさらに有することを特徴とする請求項６に記載の自動復旧方法。

【請求項１５】　前記主広帯域ネットワーク管理システムにおける故障の検出後、前記主広帯域ネットワーク管理システムの前記マネージャーオブジェクトから前記バックアップ用広帯域ネットワーク管理システムの前記エージェントオブジェクトに再起動信号を送るステップと、前記バックアップ用広帯域ネットワーク管理システムにおける前記エージェントオブジェクトから前記主広帯域ネットワーク管理システムにおける前記マネージャーオブジェクトに確認信号を送るステップと、前記主広帯域ネットワーク管理システムにおける前記エージェントオブジェクトを活性化させるステップと、前記主広帯域ネットワーク管理システムにおける前記マネージャーオブジェクトを非活性化させるステップと、前記バックアップ用広帯域ネットワーク管理システムにおける前記マネージャーオブジェクトを活性化させるステップと、前記バックアップ用広帯域ネットワーク管理システムにおける前記エージェントオブジェクトを非活性化させるステップと、前記バックアップ用広帯域ネットワーク管理システムと前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間に、コムサーバーオブジェクトを用いて前記第２のネットワーク通信リンクの形成を開始するステップとをさらに有し、正常な動作状態の下では、前記主広帯域ネットワーク管理システムにおける前記マネージャーオブジェクトと、前記バックアップ用広帯域ネットワーク管理システムにおける前記エージェントオブジェクトとが活性化されていることを特徴とする請求項６に記載の自動復旧方法。

【請求項１６】　前記バックアップ用広帯域ネットワーク管理システムと前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間に前記第２のネットワーク通信リンクを形成した後、前記バックアップ用広帯域ネットワーク管理システムと前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間の前記少なくとも一つのネットワーク通信リンクを活性化させ、これにより、前記主広帯域ネットワーク管理システムから前記バックアップ用広帯域ネットワーク管理システムに、前記広帯域ネットワークを管理する役割を切り替えるステップをさらに有することを特徴とする請求項１５に記載の自動復旧方法。

【請求項１７】　前記本来の主広帯域ネットワーク管理システムが修復された後、前記本来の主広帯域ネットワーク管理システムは、前記バックアップ用広帯域ネットワーク管理システムの役割を引き継ぐことを特徴とする請求項１６に記載の自動復旧方法。

【請求項１８】　少なくとも一つのネットワーク構成要素から成る広帯域ネットワークを管理するとともに、障害発生時には自動復旧を行うための広帯域ネットワーク管理システムにおいて、少なくとも一つのあらかじめ記憶されたインターネットプロトコルアドレスを含む第１のアドレステーブルを有する主広帯域ネットワーク管理システムと、少なくとも一つのあらかじめ記憶されたインターネットプロトコルアドレスを含む第２のアドレステーブルを有するバックアップ用広帯域ネットワーク管理システムと、前記主広帯域ネットワーク管理システムと前記広帯域ネットワークにおける前記少なくとも一つのネットワーク構成要素との間の第１のネットワーク通信リンクであって、前記第１のアドレステーブルに記憶された前記少なくとも一つのインターネットプロトコルアドレスによって規定される第１のネットワーク通信リンクと、前記バックアップ用広帯域ネットワーク管理システムと前記少なくとも一つのネットワーク構成要素との間の第２のネットワーク通信リンクであって、前記第２のアドレステーブルに記憶された前記少なくとも一つのあらかじめ記憶されたインターネットプロトコルアドレスによって規定され、前記主広帯域ネットワーク管理システムの障害時に形成される第２のネットワーク通信リンクとを有し、これにより、前記バックアップ用広帯域ネットワーク管理システムに前記広帯域ネットワークを管理する役割を引き継がせるようにしたことを特徴とする広帯域ネットワーク管理システム。

【請求項１９】　前記主広帯域ネットワーク管理システムと前記バックアップ用広帯域ネットワーク管理システムとを接続する複数個の冗長性物理リンクをさらに備えたことを特徴とする請求項１８に記載の広帯域ネットワーク管理システム。

【請求項２０】　前記バックアップ用広帯域ネットワーク管理システムの作動時には、前記バックアップ用広帯域ネットワーク管理システムは、前記主広帯域ネットワーク管理システムの役割を引き継ぐことを特徴とする請求項１８に記載の広帯域ネットワーク管理システム。

【請求項２１】　前記本来の主広帯域ネットワーク管理システムの修復時には、前記本来の主広帯域ネットワー

ク管理システムは、前記バックアップ用広帯域ネットワーク管理システムの役割を引き継ぐことを特徴とする請求項２０に記載の広帯域ネットワーク管理システム。

【請求項２２】　前記主広帯域ネットワーク管理システムと前記バックアップ用広帯域ネットワーク管理システムの両方を監視するための故障監視手段をさらに備え、前記故障監視手段は、前記主広帯域ネットワーク管理システムにおける第１の故障検出器と、前記バックアップ用広帯域ネットワーク管理システムに設けられ、前記冗長性物理リンクを越えて前記第１の故障検出器と通信するための第２の故障検出器とを有することを特徴とする請求項１８に記載の広帯域ネットワーク管理システム。

【請求項２３】　前記第１の故障検出器は、ある時点では一方のみが活性化される第１のマネージャーオブジェクトと第１のエージェントオブジェクトとを備え、前記第２の故障検出器は、第２のマネージャーオブジェクトと第２のエージェントオブジェクトとを備え、前記第１のエージェントオブジェクトが活性化されている時には前記第２のマネージャーオブジェクトが活性化され、前記第１のマネージャーオブジェクトが活性化されている時には前記第２のエージェントオブジェクトが活性化されることを特徴とする請求項２２に記載の広帯域ネットワーク管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、フォールトトレラント広帯域ネットワーク管理システムに関し、特に、壊滅的な障害の発生時に、自動復旧を行うために用いられる主（プライマリ）・バックアップ構造を有するシステムに関する。

【０００２】

【従来の技術】広帯域ネットワーク管理システム（ＢＮＭＳ）は、広帯域統合サービスデジタルネットワーク（Ｂ－ＩＳＤＮ）内のネットワーク構成要素の動作を監視し、制御するために用いられる。ネットワーク構成要素は、非同期転送モード（ＡＴＭ）スイッチとＡＴＭマルチプレクサ／コンセントレータとを含み、高速／高帯域幅でのデータ、映像、画像、音声の送信を提供する。ＡＴＭは、Ｂ－ＩＳＤＮ構造の中核を形成するパケット交換ネットワーク構造である。

【０００３】

【発明が解決しようとする課題】従来、ネットワーク管理システム（ＮＭＳ）において故障が発生した時、故障が修復されるまでネットワーク管理者はネットワークを監視し、制御することができなかった。言い換えれば、ＮＭＳはフォールトトレラントではなかった。

【０００４】最近のＮＭＳ、特にコンピュータネットワークに用いられているものは、分配型構造を採用している。分配型構造は、二つ以上の計算機を越えたＮＭＳの「処理」能力の分配を可能とする。このような構造はＮＭＳの処理能力を高めるられることを可能とするものの、フォールトトレラント能力を与えるものではない。従って、分配型構造における一つの計算機が故障すると、この計算機によって与えられていた機能は失われる。

【０００５】さらに、このような分配型構造において、ＴＣＰ／ＩＰ（送信制御プロトコル／インターネットプロトコル）リンク切り替えは、「Ｅｓｔａｂｌｉｓｈｍｅｎｔ　ｏｆ　Ｉｓｏｌａｔｅｄ　Ｆａｉｌｕｒｅ　Ｉｍｍｕｎｅ　Ｒｅａｌ－Ｔｉｍｅ　Ｃｈａｎｎｅｌｓ　ｉｎ　ＨＡＲＴＳ」１９９５年２月発行、１１３～１１９頁、および「ＴＣＰ／ＩＰ－Ｂａｓｅｄ　Ｄａｔａ　ＴｒａｎｓｐｏｒｔＳｅｒｖｉｃｅｓ　ｆｏｒ　ＬＡＮ／ＷＡＮ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ」１９９２年１月発行、１５～１７頁に記載されているように、低速で複雑なルーティングトポロジーによって行われていた。

【０００６】本発明の目的は、壊滅的な障害の発生時に、サービスを中断することなく、自動復旧を行うことができる、ＢＮＭＳのためのフォールトトレラント能力を提供することにある。

【０００７】本発明の別の目的は、簡単で、経済的で、高速のソフトウェア技術を用いたＴＣＰ／ＩＰ（送信制御プロトコル／インターネットプロトコル）リンク切り替えを組み入れた、ＢＮＭＳのためのフォールトトレラント能力を提供することにある。

【０００８】本発明の別の目的は、容易に製造することができる、ＢＮＭＳのためのフォールトトレラント能力を提供することにある。

【０００９】

【課題を解決するための手段】簡単に言えば、本発明の構造は主およびバックアップ用ＢＮＭＳに基づいており、各ＢＮＭＳにおける複製用（レプリケーション）データサーバーを介して、バックアップ用ＢＮＭＳのデータベースが主ＢＮＭＳのデータベースとの同期を維持するようにされている。また、この構造は、一組の冗長性ネットワーク通信リンク（ＮＣＬ）を用いており、これらのリンクを越えて、ＢＮＭＳがネットワーク構成要素と通信する（たとえば、命令を送る、これらの命令に対する応答を受け取る、自律メッセージを受ける、など）。主ＢＮＭＳにおける故障が、主ＢＮＭＳと広帯域ネットワーク（ＢＮ）との間の通信障害を引き起こすような場合には、バックアップ用ＢＮＭＳにはＢＮを監視し制御する動作を引き継ぐためのメカニズムが与えられる。このようなメカニズムには、バックアップ用ＢＮＭＳが、主ＢＮＭＳからバックアップ用ＢＮＭＳへ自動的にＮＣＬを切り替えるための手段が含まれている。バックアップ用ＢＮＭＳがネットワークの管理を引き継ぐと、主ＢＮＭＳの役割を引き継ぐことになる。

【００１０】本来のバックアップ用ＢＮＭＳが主ＢＮＭ

Ｓの役割を果たしているので、本来の主ＢＮＭＳが再び動作可能になった時には、これはバックアップ用ＢＮＭＳの役割を引き継ぐ。これらの役割とＮＣＬとは故障発生の都度、切り替えることができる。

【００１１】

【発明の実施の形態】図１および２は、３つのサブシステムを示す。すなわち、（１）広帯域ネットワーク（ＢＮ）１と、（２）図１に端末装置として示したグラフィカルユーザーインターフェース（ＧＵＩ）サブシステム２と、（３）ＡＴＭルータ２０を用いてＤＳ３リンクを介して、ＢＮ１に接続されるフォールトトレラントＢＮＭＳ３である。これらのサブシステムのうち３番目、すなわちＢＮＭＳ３のみが本発明に関連する。

【００１２】フォールトトレラントＢＮＭＳ３は、主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５から成る。主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５はいずれも、複製用マネージャー６と、複製用サーバー７と、ログ転送マネージャー８と、アプリケーションソフトウェア９と、第１あるいは第２のデータベースサーバー１０と、第１あるいは第２のデータベース１１とを備えている。

【００１３】立ち上げ（パワーアップ）

システム動作開始時には、広帯域ネットワーク１を監視し制御することによって主要なＢＮＭＳとして動作する主ＢＮＭＳ４が最初に立ち上げられる。再起動／心拍連結リンク（図３の連結リンク０）上でネットワーク構成要素（ＮＥ）１２から再起動を受信すると、主ＢＮＭＳ４のアプリケーションボックス内に設けられたコムマネージャー（Ｃｏｍｍａｎａｇｅｒ）オブジェクトが、主ＢＮＭＳ４と広帯域ネットワーク（ＢＮ）１との間にネットワーク通信リンク（ＮＣＬ）１３を構築する。図２および３に示されるように、ＮＣＬ１３は仮想パケット交換接続であり、２つの仮想リンク、すなわち、ＮＣＬ０（アドレスＩＰＡ１とＩＰＡＸの間にマッピングされ、ここでＩＰＡはインターネットプロトコルアドレスを表わす）と、ＮＣＬ１（アドレスＩＰＡ２とＩＰＡＹの間にマッピングされる）から成り、これらは各々、６個の連結リンク（図３に示すＡＬ）にマッピングされている。本例においては、各ＮＣＬは６つの連結リンクにマッピングされているが、このシステムを、１個のＮＣＬ１３に１２個すべての連結リンクをマッピングするように設計することも可能である。ＢＮＭＳ４、５とＢＮ１との間にＮＣＬ１３がどのようにして構築されるかは、以下に詳細に述べる。

【００１４】本発明に独自の「コムマネージャー」は、ＢＮＭＳ４、５内の数個のソフトウェアモジュール（オブジェクト）の１つである。その役割はＢＮＭＳ４、５とＢＮ１内のＮＥ１２（ＡＴＭスイッチなど）との間にメッセージ通信を構築し、管理することである。ＮＥ１２からのすべての命令およびＢＮＭＳ４、５への応答は、誤りについてメッセージをチェックし、正しいソフトウェアモジュールにこれらを分配することができるように、コムマネージャーを介して送られる。

【００１５】主ＢＮＭＳ４を立ち上げた後、バックアップ用ＢＮＭＳ５が「ウォームスタンバイ」モードで立ち上げられる。「ウォームスタンバイ」は、１＋１フォールトトレラント構造の１種であり、バックアップシステムにすべてのソフトウェアモジュールを読み込ませるものであるが、障害状態の際のシステム切り替えに必要な中核ソフトウェアモジュールと必須のアプリケーションソフトウェアモジュールだけが動作している。ソフトウェアモジュールの残りは休止したままであり、バックアップ用ＢＮＭＳ５が動作を引き継いだ後に活性化される。

【００１６】主およびバックアップ用ＢＮＭＳの同期

主ＢＮＭＳ４の障害時に、バックアップ用ＢＮＭＳ５が迅速に引き継ぐことを可能とするためには、第２のすなわちバックアップデータベース１１ｂは、主データベース１１ａとの同期を維持していなければならない。このことは主ＢＮＭＳ４におけるログ転送マネージャー８ａと、複製用マネージャー６ａと、複製用サーバー７ａと、および、バックアップ用ＢＮＭＳ５における複製用サーバー７ｂによってなされることは、当業者であれば理解できるであろう。データベーストランザクションが主ＢＮＭＳ４においてコミットされると、主ログ転送マネージャー８ａにおいてログ入力が行われる。主複製用マネージャー６ａはルーチンベースでこのログを走査し、主複製用サーバー７ａに対して、バックアップ用複製用サーバー７ｂにデータベーストランザクションを送ってバックアップ用データベース１１ｂにコピーするように命令する。

【００１７】ＢＮＭＳ監視および故障検出

図４を参照すると、主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５は、「マネージャー」１３と「エージェント」１４のソフトウェアオブジェクトに基づくフォールトトレラントメカニズムを用いて故障を監視される。これらのオブジェクトは、「生命維持シーケンス」によって、各ＢＮＭＳの健康状態をチェックする。すなわち、周期的な「心拍」メッセージ（図４において点線の矢印で示す）が、マネージャー１３とエージェント１４のソフトウェアオブジェクトとの間で送られる。

【００１８】特に、マネージャー１３とエージェント１４のソフトウェアオブジェクトは、主およびバックアップシステムのアプリケーションソフトウェア９ａ、９ｂの両方に存在する。任意の時点において、主ＢＮＭＳ４およびバックアップ用ＢＮＭＳ５の各々において、これらのオブジェクトのうちの一方のみが活性化されている。バックアップ用ＢＮＭＳ５においてはエージェント１４ｂが活性化され、主ＢＮＭＳ４においてはマネージャー１３ａが活性化されている。一方、バックアップ用ＢＮＭＳ５における対応するマネージャー１３ｂと、主

ＢＮＭＳ４におけるエージェント１４ａとは休止している。これらのオブジェクトは、相手方へ心拍メッセージを周期的に送り、周期的なベースで相手方から心拍を受け取っていることを確かめることによって、自身のシステムと相手方のシステムの「健康状態」を監視する。この心拍メッセージの交換は「ルーティングクラウド（ｒｏｕｔｉｎｇ　ｃｌｏｕｄ）」を越えて行われる。「ルーティングクラウド」とは、１つあるいはそれ以上のデータ通信ルータ１９（図２に示す）から成る広域ネットワーク（ＷＡＮ）を示すために、通信分野で用いられる専門用語である。

【００１９】主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５は、２つの冗長性物理リンク、すなわち第１の物理リンク１６（ＩＰＡ１とＩＰＡ３から成る）と第２の物理リンク１７（ＩＰＡ２とＩＰＡ４から成る）によって接続される。これらの物理リンクは二重式、すなわち双方向通信を提供するものであり、主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５のイーサネットポート（ｅｔｈｅｒｎｅｔ　ｐｏｒｔ）間に接続される。１つの物理経路の障害によってバックアップ用ＢＮＭＳ５が主ＢＮＭＳ４が故障したと判定し、不必要に「切り替え」シナリオを起動させることのないように、冗長性物理経路が用いられる。

【００２０】「生命維持シーケンス」の間、主物理リンク１６上で、バックアップ用ＢＮＭＳ５によって最初の心拍が主ＢＮＭＳ４に送られる。主ＢＮＭＳ４からバックアップ用ＢＮＭＳ５への応答は、同じ主リンク１６上を送られる。主ＢＮＭＳ４からの応答が、ソフトウェア調整可能な規定時間内に到着しない場合には、バックアップ用ＢＮＭＳ５は主リンク１６上に別の心拍を送り、主ＢＮＭＳ４からの応答を待つ。バックアップ用ＢＮＭＳ５がこの２回目の試行に際して主ＢＮＭＳ４からの応答を受け取り損なった場合には、３回目を試みる。バックアップ用ＢＮＭＳ５が依然として主ＢＮＭＳ４からの応答を受け取らない場合には、主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５との間の第２の物理リンク１７上で、この３回の試行のサイクルを繰り返す。

【００２１】バックアップ用ＢＮＭＳ５が、主ＢＮＭＳ４からの心拍を６回連続して受け取り損なった場合には、以下に述べるように、主ＢＮＭＳ４が故障していると推定し、ＮＣＬ１３をネットワーク構成要素１２にセットアップすることによって主ＢＮＭＳ４の役割を引き継ぐ。一方、主ＢＮＭＳ４が６回連続して（２つの冗長性物理リンク１６、１７の各々において３回）バックアップ用ＢＮＭＳ５からの心拍メッセージを受け取り損なった場合には、ネットワーク管理者が適切な処置をとることができるように、アラームを発生してバックアップ用ＢＮＭＳ５における問題についてネットワーク管理者に知らせる。

【００２２】マネージャー／エージェント式フォールトトレラントメカニズムは公知であるが、一方が活性化されている間、他方は休止しているような一対のオブジェクトとしてこれらを用いることは、本発明に独自のものであると考えられる。

【００２３】各物理リンク１６、１７上での試行の回数はソフトウェア調整可能であるが、最低限２回、各物理リンク上で１回は必要である。複数回試行する理由は、通信上の問題が短時間しか続かないことがあるからである。この技術の使用により、このような一過性の問題のために主ＢＮＭＳ４とバックアップ用ＢＮＭＳ５との間で不必要な切り替えが起こることが回避される。

【００２４】ＢＮＭＳ４、５内の故障はソフトウェア関連のものかもしれないし、ハードウェア関連であるかもしれない。主ＢＮＭＳ４におけるいかなる壊滅的なソフトウェア障害も、オペレーティングシステムや中核的ソフトウェアによって検出され、主ＢＮＭＳ４内のマネージャーオブジェクト１３ａにそのような障害が知らせられる。すると、マネージャーオブジェクト１３ａは、主ＢＮＭＳ４のコムマネージャーオブジェクトを遮断し、バックアップ用ＢＮＭＳ５のエージェントオブジェクト１４ｂに再起動メッセージを送る。コムマネージャーオブジェクトを遮断した結果、主ＢＮＭＳ４とＢＮ１間のＮＣＬ１３による通信は（瞬間的に）失われ、次節で述べる復旧プロセスが開始する。

【００２５】主ＢＮＭＳ４がハードウェアの故障を発生していれば、主ＢＮＭＳ４からバックアップ用５への“心拍”通信は失われる。心拍通信が停止するのは、主ＢＮＭＳ４におけるオペレーティングシステムと、中核的ソフトウェアと、マネージャーオブジェクト１３ａがハードウェア故障のために機能を停止するからである。その結果、バックアップ用ＢＮＭＳ５におけるエージェントオブジェクト１４ｂは、主ＢＮＭＳ４からの６回連続の心拍メッセージ（この数はソフトウェア調整可能である）を受け取り損ない、主ＢＮＭＳ４が故障していると推定し、次節で述べる復旧プロセスを開始する。

【００２６】壊滅的な障害のいくつかの例として、ａ）オブジェクトを復活させるための３回の試行の後もソフトウェアオブジェクトが引き続き停止したままであること、ｂ）オペレーティングシステムや中核的ソフトウェア自身の障害、ｃ）データベースシステムの構成要素（ログ転送マネージャー、複製用サーバー、データ記憶ハードディスクシステム）のいずれかの障害、ｄ）ＢＮＭＳ内のプロセッサの障害、ｅ）ＢＮＭＳ内のメモリの障害、が挙げられる。

【００２７】故障検出後の切り替え

本発明の独自の態様は、主ＢＮＭＳ４における故障の検出後に行われる復旧手順にある。バックアップ用ＢＮＭＳ５におけるエージェントオブジェクト１４ｂが、主ＢＮＭＳ４におけるマネージャーオブジェクト１３ａからの再起動信号を受信した時（先に述べたソフトウェア障

害の場合のように）、あるいは、エージェントオブジェクト１４ｂが、６回連続の心拍メッセージを受け損なった時（先に述べたハードウェア故障の場合のように）のいずれかの場合に、復旧手順が開始される。

【００２８】第１の場合において、再起動信号を受信すると、バックアップ用ＢＮＭＳ５内のエージェントオブジェクト１４ｂが再起動メッセージの受領を確認し、バックアップ用ＢＮＭＳ５内の休止中のコムマネージャーオブジェクトを活性化させる（これは、主ＢＮＭＳ４内のコムマネージャーが活動している間、休止していた）。主ＢＮＭＳ４内のマネージャーオブジェクト１３ａがバックアップ用ＢＮＭＳ５内のエージェントオブジェクト１４ｂから再起動確認を受け取り次第、これは休止状態になり、主ＢＮＭＳ４内のエージェントオブジェクト１４ａが活性化される。

【００２９】バックアップ用ＢＮＭＳ５内のエージェント１４ｂが、６回連続の心拍メッセージを受け損なったことから、主ＢＮＭＳ４における故障を検出する第２の場合において、再起動／確認プロセスは抜かされ、バックアップ用ＢＮＭＳ５内のエージェント１４ｂは、バックアップ用ＢＮＭＳ内のコムマネージャーオブジェクトを直ちに活性化させる。

【００３０】バックアップ用ＢＮＭＳ５内の活性化されたコムマネージャーは、バックアップ用ＢＮＭＳ５のソフトウェアおよびハードウェアと、個々のＮＥ１２の間の相互作用の組み合わせによって、バックアップ用ＢＮＭＳ５とＢＮ１内のたとえばＡＴＭスイッチなどの各ＮＥ１２の間に新規のＮＣＬ接続１３を創設する。図２および３を参照すると、このプロセスは、バックアップ用ＢＮＭＳ５内でコムマネージャーがコムサーバー１８ｂを形成することによって開始される。説明の簡単のため、ＢＮ１内の各ＮＥ１２に対し１つのコムサーバー１８ｂが設けられるものとする。コムサーバー１８の機能は、１３ＴＣＰ／ＩＰ（送信制御プロトコル／インターネットプロトコル）連結リンクを管理することである。各ＮＣＬ１３は、バックアップ用ＢＮＭＳ５内のコムサーバー１８ｂと対応するＮＥ１２（図２および３に示されるＡＴＭスイッチ）の間の１２個のＴＣＰ／ＩＰ連結リンクのグループから成る。

【００３１】当業者であれば理解されるように、これらの連結リンクは、バックアップ用ＢＮＭＳ５内のイーサネットポートと、ＮＥ１２におけるゲートウェイＰＡＤ（ＧＷＰＡＤ、これについてはさらに後述する）と呼ばれる特別な通信ハードウェアと、バックアップ用ＢＮＭＳ５およびＮＥ１２内の通信プロトコルソフトウェアとを用いてセットアップされる。これらの１２個の連結リンクのうち、４つはバックアップ用ＢＮＭＳ５とＮＥ１２との間のＣＭＩＰ（共通管理情報プロトコル）メッセージに使用され、４つはバックアップ用ＢＮＭＳ５とＮＥ１２との間のＦＴＡＭ（ファイル転送アクセス方式）メッセージに使用され、４つはＮＥ１２からバックアップ用ＢＮＭＳ５へのアラーム／事象メッセージに使用される。

【００３２】コムサーバー１８ｂの形成後、バックアップ用ＢＮＭＳ５内のコムマネージャーは、主ＢＮＭＳ４内のコムマネージャーに記憶されたアドレスＩＰＡ１およびＩＰＡ２に代えて、バックアップ用ＢＮＭＳ５のコムマネージャーに記憶されたアドレスＩＰＡ３およびＩＰＡ４を用いることにより、ＢＮ１内の各ＮＥ１２に対して新規のＮＣＬ０／１接続１３をセットアップする。

【００３３】ＩＰアドレスＩＰＡ１およびＩＰＡ２は、主ＢＮＭＳ４のコムマネージャー内部のテーブルにあらかじめ記憶され、ＩＰアドレスＩＰＡ３およびＩＰＡ４は、バックアップ用ＢＮＭＳ５のコムマネージャー内部のテーブルにあらかじめ記憶されている。すなわち、主ＢＮＭＳ４内にあらかじめ記憶されたアドレスＩＰＡ１およびＩＰＡ２に代えて、バックアップ用ＢＮＭＳ５内にあらかじめ記憶されたアドレスＩＰＡ３およびＩＰＡ４を用いるだけで、ＮＣＬ１３を、主ＢＮＭＳ４（ＩＰＡ１からＩＰＡＸにマッピングされたＮＣＬ０、ＩＰＡ１からＩＰＡＹにマッピングされたＮＣＬ１）から、バックアップ用ＢＮＭＳ５（ＩＰＡ３からＩＰＡＸにマッピングされたＮＣＬ０、ＩＰＡ４からＩＰＡＹにマッピングされたＮＣＬ１）へ容易に切り替えることができる。図３において、実線矢印のＮＣＬは切り替え前のＮＣＬを表わし、点線矢印のＮＣＬは切り替え後のＮＣＬを表わす。本発明によるＮＣＬ切り替えのこのプロセスは、従来技術の低速かつ複雑なルーティングトポロジーに比べて高速かつ簡単である。

【００３４】バックアップ用ＢＮＭＳ５とＢＮ１との間の通信が首尾よく構築された後、バックアップ用ＢＮＭＳ５内のマネージャーオブジェクト１３ｂが活性化され、エージェントオブジェクト１４ｂは休止状態になる。ＮＣＬ１３と１２個の連結リンクは活性化され、バックアップ用ＢＮＭＳ５は、ＢＮ１を監視し制御することによって主ＢＮＭＳの役割を引き継ぎ、本来のバックアップ用ＢＮＭＳ５の役割は主ＢＮＭＳの役割へと切り替わる。

【００３５】本来の主ＢＮＭＳ４が修復されると、そのエージェントオブジェクト１４ａを活性化させ、マネージャーオブジェクト１３ａを休止させたままにしておくことによって、バックアップ用ＢＮＭＳの役割を引き継ぐ。主およびバックアップ用ＢＮＭＳの間のこの役割の切り替えは、このようにして無限に行い得る。何らかの理由でバックアップ用ＢＮＭＳ５とＢＮ１との間にＮＣＬ通信１３が構築できない場合には、ネットワーク管理者が適切な手動での修復処置をとることができるようにアラームを発生させる。

【００３６】主／バックアップ用ＢＮＭＳの切り替えは、障害が発生した時の主ＢＮＭＳ４の状態とは無関係

13

である。言い換えれば、主ＢＮＭＳ４が命令を送信中、命令に対する応答を受信中、アラームあるいは事象メッセージの受信中、あるいは単に待機中のどの状態で障害が発生しても、バックアップ用ＢＮＭＳ５のとる処置は同じである。

【００３７】ここで、ＧＷＰＡＤは、公知のパケット組立／分解装置であり、ＢＮ１内のＮＥ１２のそれぞれに設けられている。ＢＮＭＳによって送られた命令は、ＡＴＭ（非同期転送モード）セルとしてＮＥ１２によって受信される。（ＮＥＣはこの技術を使用している。Ｘ．２５やＩＰＸデータパケットなどのその他の技術は、ＢＮＭＳとＢＮの間でこのような通信を実行するために他のベンダーによって使用される。）これらのセルはＧＷＰＡＤによって受け取られ、メッセージに変換されてＮＥ１２内のソフトウェアによって分析される。同様に、ＮＥ１２によって送られた応答やアラームメッセージ

14

は、まずＧＷＰＡＤに送られ、そこでＡＴＭセルに分解されてＢＮＭＳ４、５に送られる。

【００３８】以上、本発明について具体的に図示し好ましい実施例を用いて説明してきたが、添付の請求項の趣旨および範囲内で本発明を修正して実施することが可能であるということは、当業者には明らかであろう。

【図面の簡単な説明】

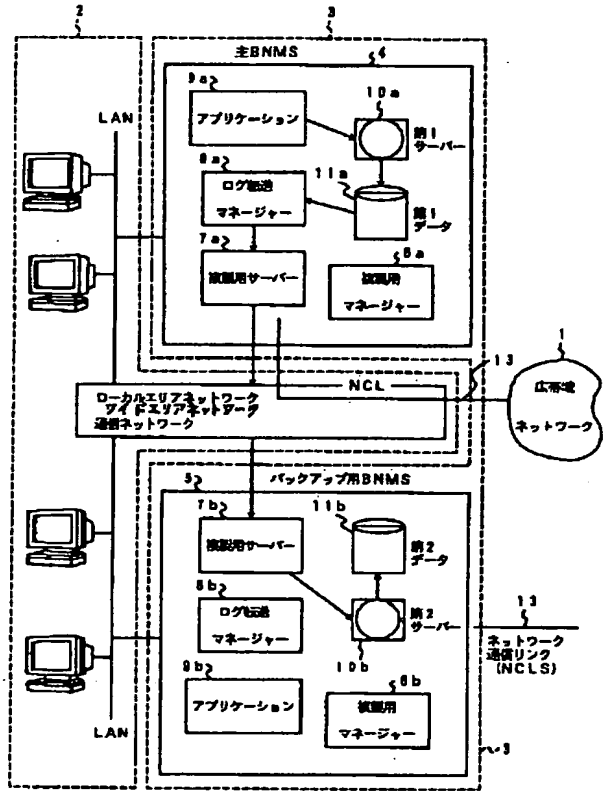
【図１】本発明によるフォールトトレラント広帯域ネットワーク管理システムを示す図である。

【図２】本発明によるフォールトトレラント広帯域ネットワーク管理システムを示す図である。

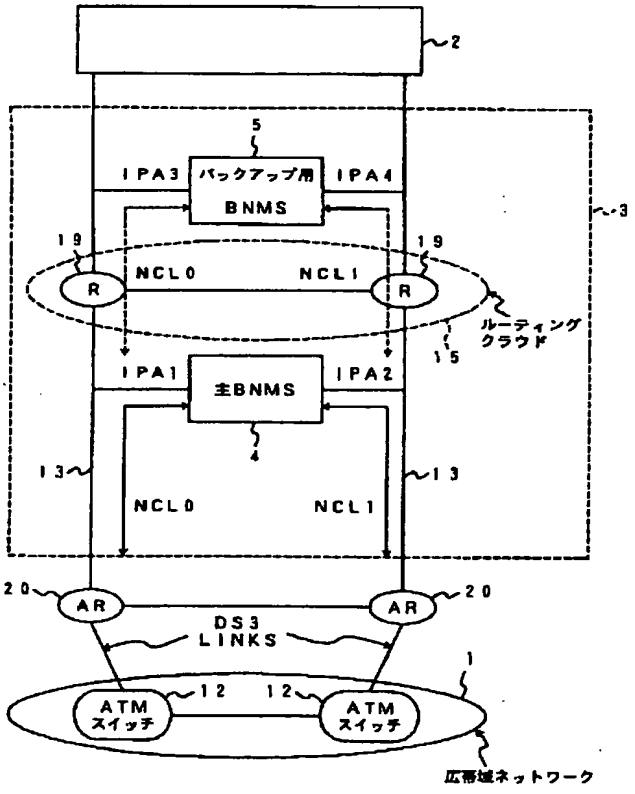
【図３】広帯域ネットワーク管理システムとＡＴＭスイッチの間の接続を示す図である。

【図４】本発明による“マネージャー”および“エージェント”ソフトウェアオブジェクトを示す図である。

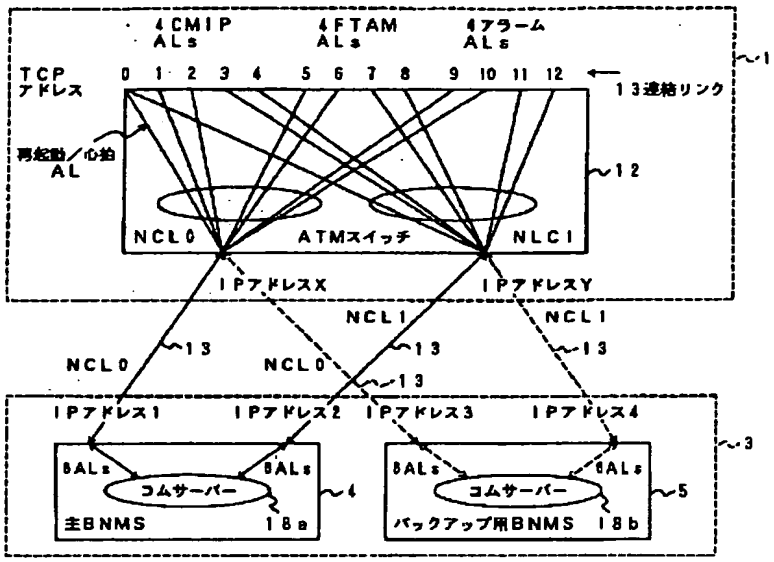
【図１】



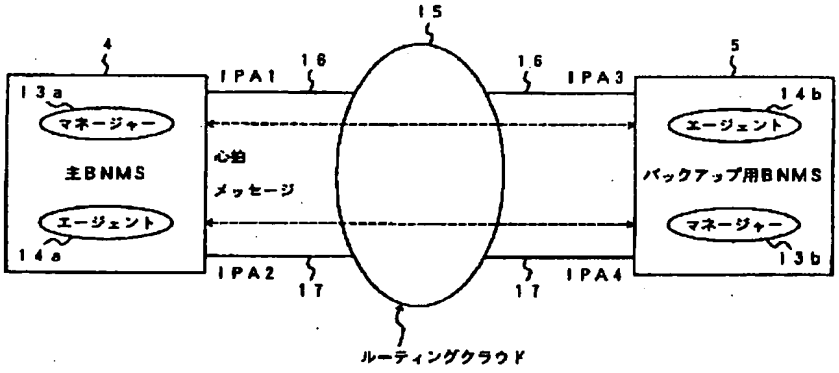
【図２】



【図３】


4 CMIP ALs
4 FTAM ALs
4 アラーム ALs
1
TCP アドレス
0 1 2 3 4 5 6 7 8 9 10 11 12
13 連結リンク
再起動／心拍 AL
12
NCL 0
ATMスイッチ
NCL 1
IPアドレスX
IPアドレスY
NCL 1
NCL 1
NCL 0
13
NCL 0
13
13
13
IPアドレス1
IPアドレス2
IPアドレス3
IPアドレス4
3
8ALs
8ALs
コムサーバー
4
主BNMS
18a
8ALs
8ALs
コムサーバー
5
バックアップ用BNMS
18b

【図４】


15
4
5
13a
マネージャー
主BNMS
エージェント
14a
IPA1
16
16
IPA3
心拍
メッセージ
IPA2
17
17
IPA4
14b
エージェント
バックアップ用BNMS
マネージャー
13b
ルーティングクラウド

【外国語明細書】

1. Title of Invention

FAULT TOLERANT BROADBAND NETWORK MANAGEMENT SYSTEM

2. Claims

1. In a broadband network management system having a primary broadband network management system for managing through a first network communication link a broadband network made up of at least one network element, and having a backup broadband network management system interfacing with said primary broadband network management system, a method for providing automatic recovery in response to a fault condition in the primary management system, comprising the steps of:

creating a second network communication link between said backup broadband network management system and said at least one network element in said broadband network in response to the fault condition in the primary broadband network management system;

activating the backup broadband network management system so that it takes over the role of managing the broadband network through the second network communication link.

2. A method for providing automatic recovery as in claim 1, prior to startup of the broadband network management system, including the further steps of:

prestoring at least one internet protocol address in a first table located in the primary network management system;

prestoring at least one internet protocol address in a second table located in the backup network management system.

3. A method for providing automatic recovery as in claim 2, wherein the first network communication link is defined by the at least one internet protocol address stored in the first table in the primary network management system; and

wherein the second network communication link is created using the at least one internet protocol address stored in the table in the backup broadband network management system.

4. A method for providing automatic recovery as in claim 1, wherein upon activation of the backup broadband network management system, the backup broadband network management system assumes the role of the original primary broadband network management system.

5. A method for providing automatic recovery as in claim 4, wherein upon correction of the original primary broadband network management system, the original primary broadband network

management system assumes the role of the backup broadband network management system.

6. A method for providing automatic recovery as in claim 1, further comprising the steps of:

monitoring both the primary broadband network management system and the backup broadband network management system for faults using fault tolerant mechanisms based on manager and agent objects which reside both in the primary broadband network management system and in the backup broadband network management system.

7. A method for providing automatic recovery as in claim 6, further comprising the steps of:

sending periodic heartbeat messages between the manager object in the primary broadband network management system and the agent object in the backup broadband network management system.

8. A method for providing automatic recovery as in claim 7, further comprising the steps of:

detecting a fault condition in the primary broadband network management system when the agent object in the backup broadband network management system fails to receive a heartbeat on a periodic basis.

9. A method for providing automatic recovery as in claim 6, wherein within each of the primary broadband network management system and the backup broadband network management system, only one of the manager object and the agent object is active at any given time.

10. A method for providing automatic recovery as in claim 8, after detection of a fault condition in the primary broadband network management system, further comprising the steps of:

activating the agent object in the primary broadband network management system;

deactivating the manager object in the primary broadband network management system;

activating the manager object in the backup broadband network management system;

deactivating the agent object in the backup broadband network management system; and

initiating the creation of said second network communication link between the backup broadband network management system and said at least one network element in the broadband network using a commserver object;

wherein under normal operating conditions, the manager object in the primary broadband network management system and the agent object in the backup broadband network management system are active.

11. A method for providing automatic recovery as in claim 10, after creating said second network communication link between the backup broadband network management system and said at least one network element in the broadband network, further comprising the step of:

activating the at least one network communication link between the backup broadband network management system and said at least one network element in the broadband network, thereby switching the role of managing the broadband network from the primary broadband network management system to the backup broadband network management system.

12. A method for providing automatic recovery as in claim 11, wherein after the original primary broadband network management system is corrected, the original primary broadband network management system assumes the role of the backup broadband network management system.

13. A method for providing automatic recovery as in claim 7, wherein the heartbeat messages are sent via a plurality of reduhdant physical links.

14. A method for providing automatic recovery as in claim 6, further comprising the step of raising an alarm when a fault is detected in the backup broadband network management system.

15. A method for providing automatic recovery as in claim 6, after detection of a fault in the primary broadband network management system, further comprising the steps of:

sending a restart signal from the manager object in the primary broadband network management system to the agent object in the backup broadband network management system;

sending an acknowledgment signal from the agent object in the backup broadband network management system to the manager object in the primary broadband network management system;

activating the agent object in the primary broadband network management system;

deactivating the manager object in the primary broadband network management system;

activating the manager object in the backup broadband network management system;

deactivating the agent object in the backup broadband network management system; and

initiating the creation of said second network communication link between the backup broadband network management system and said at least one network element in the broadband network using a commserver object;

wherein under normal operating conditions, the manager object in the primary broadband network management system and the agent object in the backup broadband network management system are active.

16. A method for providing automatic recovery as in claim 15, after creating said second network communication link between the backup broadband network management system and said at least one network element in the broadband network, further comprising the step of:

activating the at least one network communication link between the backup broadband network management system and said at least one network element in the broadband network, thereby switching the role of managing the broadband network from the primary broadband network management system to the backup broadband network management system.

17. A method for providing automatic recovery as in claim 16, wherein after the original primary broadband network management system is corrected, the original primary broadband network management system assumes the role of the backup broadband network management system.

18. A broadband network management system for managing a broadband network made up of at least one network element, and for providing automatic recovery in the event of a failure, comprising:

a primary broadband network management system having a first address table containing at least one pre-stored internet protocol address;

a backup broadband network management system having a second address table containing at least one pre-stored internet protocol address;

a first network communication link between said primary broadband network management system and said at least one network element in said broadband network;

said first network communication link being defined by said at least one pre-stored internet protocol address stored in said first address table; and

a second network communication link between said backup broadband network management system and said at least one network element, said second network communication link being defined by said at least one pre-stored internet protocol address stored in said second address table, and being created upon failure of the primary broadband network management system;

thereby causing the backup broadband network management system to take over the role of managing the broadband network.

19. The broadband network management system as in claim 18, further comprising:

a plurality of redundant physical links connecting said primary broadband network management system and said backup broadband network management system.

20. The broadband network management system as in claim 18, wherein upon activation of the backup broadband network management system, the backup broadband network management system assumes the role of the primary broadband network management system.

21. The broadband network management system as in claim 20, whereupon correction of the original primary broadband network management system, the original primary broadband network management system assumes the role of the backup broadband network management system.

22. The broadband network management system as in claim 18, further comprising:

a fault monitoring means for monitoring both the primary broadband network management system and the backup broadband network management system for faults;

said fault monitoring means comprising:

a first fault detector in said primary broadband network management system; and

a second fault detector in said backup broadband network management system for communicating with said first fault detector over said redundant physical links.

23. The broadband network management system as in claim 22, wherein said first fault detector comprises a first manager object

and a first agent object, only one of which is active at a time; and

wherein said second fault detector comprises a second manager object and a second agent object, said second manager object being active when said first agent object is active, said second agent object being active when said first manager object is active. --

3. Detailed Description of Invention

Field of the Invention

This invention relates to a fault tolerant broadband network management system, and more particularly to a system having primary and backup architecture used to effect automatic recovery in the event of a catastrophic failure.

Description of the Prior Art

Broadband Network Management Systems (BNMS) are used to monitor and control the operation of the network elements within a Broadband Integrated Services Digital Network (B-ISDN). The network elements, which include Asynchronous Transfer Mode (ATM) switches and ATM multiplexors/concentrators, provide high-speed/high bandwidth data, video, image, and voice transmission. ATM is a packet-switched network architecture which forms the core of the B-ISDN architecture.

In the past, when a fault occurred in a Network Management System (NMS), the network administrators lost the capability to monitor and control the network until the fault was corrected. In other words, the NMS was not fault tolerant.

Recent NMSs, especially those used in computer networks, employ "distributed" architecture. Distributed architectures allow for distribution of the NMS's "processing" capability over more than

one computing machine. While such architectures allow for increasing the processing power of NMS, they do not provide fault tolerant capabilities. Thus, if one of the machines in the distributed architecture fails, then the functionality provided by that machine is lost.

Moreover, in these distributed architectures, TCP/IP (Transmission Control Protocol / Internet Protocol) link switching was performed by slow and complicated routing topologies such as those described in "Establishment of Isolated Failure Immune Real-Time Channels in HARTS", February 1995, pp.113-119, and "TCP/IP-Based Data Transport Services for LAN/WAN Interconnection", January 1992, pp. 15-17.

An object of this invention is the provision of fault tolerant capability for BNMS which can effect automatic recovery, without disruption of service, in the event of a catastrophic failure.

Another object of this invention is the provision of fault tolerant capability for BNMS that incorporates TCP/IP (Transmission Control Protocol / Internet Protocol) link switching which uses software techniques which are simple, cheap, and fast.

Another object of this invention is the provision of fault tolerant capability for BNMS that can be easily manufactured.

Briefly, the architecture of this invention is based on a primary and backup BNMS in which the database in the backup BNMS is kept synchronized with that of the primary BNMS via replication data servers in each BNMS. The architecture also uses a set of redundant Network Communication Links (NCLs) over which the BNMS communicates with the network elements (e.g., sends commands, receives responses to those commands, as well as receives autonomous messages). If there is a fault in the primary BNMS causing a failure of communication between the primary BNMS and the Broadband Network (BN), mechanisms are provided for the backup BNMS to take over the operation of monitoring and controlling the BN. Included within these mechanisms are means for the backup BNMS to switch over the NCLs from the primary BNMS to the backup BNMS automatically. When the backup BNMS takes over the management of the network, it assumes the primary BNMS role.

When the original primary BNMS becomes operational again, it assumes the role of the backup BNMS, since the original backup BNMS has assumed the primary BNMS role. These roles as well

as the NCLs can be switched for each occurrence of a fault.

FIGS. 1 and 2 show three subsystems: (1) the Broadband Network (BN) 1, (2) the Graphical User Interface (GUI) subsystem 2 shown as terminals in FIG. 1, and (3) the Fault Tolerant BNMS 3 which is connected to the BN 1 through DS3 links using ATM routers 20. Only the third of the subsystems, the BNMS 3, is germane to this invention.

The Fault Tolerant BNMS 3 consists of a primary BNMS 4 and a backup BNMS 5. Both the

primary BNMS 4 and the backup BNMS 5 include a replication manager 6, replication server 7, log transfer manager 8, application software 9, primary or secondary database server 10, and primary or secondary database 11.

Powerup

At the beginning of system operation, the primary BNMS 4, which operates as the main BNMS by monitoring and controlling the broadband network 1, is powered up first. Upon receiving a restart from a network element (NE) 12 on the restart/heartbeat association link (association link 0 in FIG. 3), the Commanager object, which is located within the applications box of the primary BNMS 4, establishes Network Communication Links (NCLs) 13 between the primary BNMS 4 and the Broadband Network (BN) 1. As shown in Figures 2 and 3, the NCL 13 is a virtual packet switched connection and consists of two virtual links, NCL0 (mapped between addresses IPA1 and IPAX, where IPA stands for Internet Protocol Address) and NCL1 (mapped between addresses IPA2 and IPAY), each of which map to six association links (ALs, shown in FIG. 3). In this example, each NCL maps to six association links, however, the system can be designed such that all twelve association links map to a single NCL 13. The details of how the NCLs 13 are established

between a BNMS 4,5 and the BN 1 will be explained further below.

"Commanager", which is unique to this invention, is one of the several software modules (objects) within a BNMS 4,5. Its role is to establish and manage message communication between the BNMS 4,5 and the NEs 12 (ATM switches, etc.) within the BN 1. All commands from and responses to the BNMS 4,5 from the NEs 12 are funneled via the Commanager so that it can check messages for errors, as well as distribute them to the correct software module.

After the primary BNMS 4 is powered up, the backup BNMS 5 is powered up in the "warm standby" mode. "Warm standby" is a type of 1+1 fault tolerant architecture in which a backup system is loaded with all software modules, but only the core software modules and essential application software modules needed for system switchover during failure conditions are operating. The rest of the software modules are dormant, and are activated after the backup BNMS 5 takes over the operation.

Synchronization of Primary and Backup BNMS

In order for the backup BNMS 5 to be able to quickly take over upon failure of the primary BNMS 4, the secondary, or backup, database 11b must be kept synchronized with the primary database 11a. One of ordinary skill would appreciate that this is

done via the Log Transfer Manager 8a, Replication Manager 6a, and Replication Server 7a in the primary BNMS 4, and the Replication Server 7b in the backup BNMS 5. When a database transaction is committed in the primary 4, a log entry is made in the primary Log Transfer Manager 8a. The primary Replication Manager 6a scans this log on a routine basis and commands the primary Replication Server 7a to send the database transaction to the backup Replication Server 7b to be copied into the backup database 11b.

BNMS Monitoring and Fault Detection

Referring to FIG. 4, the primary BNMS 4 and backup BNMS 5 are monitored for faults using fault tolerant mechanisms based on "manager" 13 and "agent" 14 software objects. These objects check the health of each BNMS via a "keep alive sequence" in which periodic "heartbeat" messages (represented by the arrowed dotted lines in FIG. 4) are sent between the manager 13 and the agent 14 software objects.

More specifically, manager 13 and agent 14 software objects reside both in the primary and in the backup system application software, 9a,9b. Only one of these objects is active within each of the primary BNMS 4 and backup BNMS 5 at any given time. The agent 14b is active in the backup BNMS 5 and the manager 13a is active in the primary BNMS

4, while the corresponding manager 13b in the backup BNMS 5 and the agent 14a in the primary BNMS 4 are dormant. These objects monitor the "health" of their system as well as of their mate system by periodically sending a heartbeat message to the mate and making sure that they receive a heartbeat from the mate on a periodic basis. This heartbeat message exchange takes place over a "routing cloud" 15. "Routing cloud" is a terminology used in the communications field to indicate a Wide Area Network (WAN) consisting of one or more data communication routers 19 (shown in FIG. 2).

The primary BNMS 4 and the backup BNMS 5 are connected by two redundant physical links, a primary 16 (consisting of IPA1 and IPA3) and a secondary 17 physical link (consisting of IPA2 and IPA4). These physical links are duplex; i.e. they provide two-way communications, and are connected between the ethernet ports in the primary BNMS 4 and the backup BNMS 5. Redundant physical paths are used so that failure of one physical path does not cause the backup BNMS 5 to conclude that the primary BNMS 4 is faulty and unnecessarily start the "switchover" scenario.

During the "keep alive sequence", the first heartbeat is sent by the backup BNMS 5 to the primary BNMS 4 on the primary physical link 16. The response from the primary BNMS 4 to the backup

BNMS 5 is sent over the same primary link 16. If the response from the primary BNMS 4 does not come within a stipulated period of time, which is software adjustable, the backup BNMS 5 sends another heartbeat on the primary link 16 and awaits a response from the primary BNMS 4. If the backup BNMS 5 fails to receive a response from the primary BNMS 4 on this second attempt, it tries for a third time. If the backup BNMS 5 still does not receive a response from the primary BNMS 4, it will then repeat this cycle of three attempts on the secondary physical link 17 between the primary BNMS 4 and backup BNMS 5.

If the backup BNMS 5 fails to receive the heartbeat from the primary BNMS 4 six times in a row, then it assumes that the primary BNMS 4 is faulty and takes over the role of the primary BNMS 4 by setting up NCLs 13 to the network elements 12, as will be described further below. On the other hand, if the primary BNMS 4 fails to receive the heartbeat message six times in a row from the backup BNMS 5 (three times on each of the two redundant physical links 16,17), it raises an alarm to let the network administrator know about the problem in the backup BNMS 5 so that the network administrator can take appropriate measures.

While the manager/agent fault tolerant mechanisms are known in the art, using them as a

pair of objects in which one is active while the other is dormant is believed to be unique to this invention.

The number of attempts on each physical link 16,17 is software adjustable, but there must be a minimum of two, one on each physical link. The reason for the multiple attempts is that sometimes communication problems are of a short duration. Using this technique avoids unnecessary switchover between primary BNMS 4 and backup BNMS 5 due to such transient problems.

The faults within the BNMS 4,5 may be software or hardware related. Any catastrophic software failures in the primary BNMS 4 are detected by the operating system or the core software which inform the Manager object 13a within the primary BNMS 4 of such failures. The Manager object 13a then shuts off the Commanager object in the primary BNMS 4 and sends a restart message to the agent object 14b in the backup BNMS 5. As a result of shutting off the Commanager object, NCL 13 communication between the primary BNMS 4 and the BN 1 is lost (momentarily), and the recovery process which is described in the next section begins.

If the primary BNMS 4 develops a hardware fault, the "heartbeat" communication from the primary BNMS 4 to the backup 5 is lost. The heartbeat communication stops since the operating

system, core software, and the Manager object 13a in the primary BNMS 4 stop functioning due to the hardware fault. As a result, the Agent object 14b in the backup BNMS 5 fails to receive six consecutive heartbeat messages (the number is software adjustable) from the primary BNMS 4, assumes that the primary BNMS 4 is faulty, and begins the recovery process described in the next section.

Some examples of catastrophic failures include: a) software object continues to fail after three attempts to "revive" the object, b) failure of operating system and core software itself, c) failure of any of the components of the database system (Log Transfer Manager, Replication Server, Data storage hard disk system), d) failure of processor within BNMS, and e) failure of memory within BNMS.

Switchover After Fault Detection

A unique aspect of this invention lies in the recovery procedure which occurs after detection of a fault in the primary BNMS 4. The recovery procedure can be triggered either when the Agent object 14b in the backup BNMS 5 receives the restart signal from the Manager object 13a in the primary BNMS 4 (as in the case of a software failure described earlier), or when the Agent object 14b fails to receive six consecutive

heartbeat messages (as in the case of a hardware fault described earlier).

In the first case, where the restart signal is received, the Agent object 14b in the backup BNMS 5 acknowledges the receipt of the restart message and activates the dormant Commanager object in the backup BNMS 5 (it was dormant while the Commanager object in the primary BNMS 4 was alive). As soon as the Manager object 13a in the primary BNMS 4 receives the restart acknowledgement from the Agent object 14b in the backup BNMS 5, it goes dormant and the Agent object 14a in the primary BNMS 4 is made active.

In the second case, where the agent 14b in the backup BNMS 5 detects a fault in the primary BNMS 4 due to failure to receive six consecutive heartbeat messages, the restart/acknowledgment process is bypassed and the agent 14b in the backup BNMS 5 immediately activates the Commanager object in the backup BNMS 5.

The activated Commanager in the backup BNMS 5 initiates new NCL connections 13 between the backup BNMS 5 and each NE 12, i.e. ATM switch(s), in the BN 1 by a combination of interworking between the software and hardware of the backup BNMS 5 and the individual NEs 12. Referring to FIGS. 2 and 3, the process is started by the Commanager creating commservers 18b within the backup BNMS 5; for

simplicity, one commserver 18b for each NE 12 in the BN 1. The function of the commservers 18 is to manage the 13 TCP/IP (Transmission Control Protocol / Internet Protocol) association links. Each NCL 13 consists of a group of twelve TCP/IP association links between commservers 18b within the backup BNMS 5 and the corresponding NE 12 (ATM switch shown in FIGS. 2 and 3).

As one of skill in the art would appreciate, these association links are set up using ethernet ports within the backup BNMS 5, special communication hardware called Gateway PAD (GWPAD, which is further explained below) in the NEs 12, and communication protocol software within the backup BNMS 5 and the NEs 12. Of these twelve association links, four are used for CMIP (Common Management Information Protocol) messages between the backup BNMS 5 and NEs 12, four are used for FTAM (File Transfer Access Method) messages between the backup BNMS 5 and NEs 12 and four are used for Alarm/Event Messages from the NEs 12 to the backup BNMS 5.

After creating the commservers 18b, the Commanager in the backup BNMS 5 sets up new NCL0/1 connections 13 to each NE 12 within the BN 1 by using the addresses IPA3 and IPA4 stored in the Commanager in the backup BNMS 5, rather than the

addresses IPA1 and IPA2 stored in the Commanager in the primary BNMS 4.

The IP addresses IPA1 and IPA2 are pre-stored in tables inside the Commanagers in the primary BNMS 4, and the IP addresses IPA3 and IPA4 are pre-stored in tables inside the Commanagers in the backup BNMS 5. Thus, by merely using the addresses IPA3 and IPA4 which are pre-stored in the backup BNMS 5 rather than the addresses IPA1 and IPA2 which are pre-stored in the primary BNMS 4, the NCLs 13 can be easily switched from the primary BNMS 4 (NCL0 mapped from IPA1 to IPAX; NCL1 mapped from IPA2 to IPAY) to the backup BNMS 5 (NCL0 mapped from IPA3 to IPAX; NCL1 mapped from IPA4 to IPAY). In FIG. 3, the solid NCL arrowed lines represent the NCLs before switchover, the dotted NCL arrowed lines represent the NCLs after switchover. This process of switching the NCLs according to the present invention is much faster and simpler that the slow and complicated routing prior art topologies.

After the communications between the backup BNMS 5 and the BN 1 are successfully established, the Manager object 13b in the backup BNMS 5 is made active and the Agent object 14b goes dormant. The NCLs 13 and twelve association links are made active, and the backup BNMS 5 assumes the role of the primary BNMS by monitoring and controlling the

BN 1, thus switching the role of the original backup BNMS 5 to the primary BNMS role.

When the original primary 4 BNMS is corrected, it assumes the role of the backup BNMS by activating its Agent object 14a and leaving its Manager object 13a dormant. This switching of roles between the primary and backup BNMS can thus occur ad infinitum. If for any reason, the NCL communications 13 between the backup BNMS 5 and the BN 1 can not be established, alarms are raised so that the network administrators can take appropriate manual corrective actions.

The primary/backup BNMS switchover is independent of the state of the primary BNMS 4 when the failure occurs. In other words, the actions taken by the backup BNMS 5 are identical if the failure occurs while the primary BNMS 4 is sending a command, receiving a response to a command, receiving an alarm or event message, or just idling.

Note that GWPAD is a known packet assembler/dis-assembler and is located within each of the NEs 12 in the BN 1. The commands sent by the BNMS are received as ATM (Asynchronous Transfer Mode) cells by the NEs 12. (NEC uses this technology. Other technologies such as X.25 or IPX data packets could be used by other vendors to perform such communication between the BNMS and the

BN.) These cells are received by the GWPAD and converted into messages which are analyzed by the software within the NEs 12. Similarly, responses and alarm messages sent by NEs 12 are first sent to GWPAD, which then breaks them into ATM cells to be sent to the BNMS 4,5.

While the invention has been particularly shown and described with respect to a preferred embodiment thereof, it will be understood by those skilled in the art that the invention can be practiced with modification within the spirit and scope of the appended claims.

4. Brief Description of Drawings

The foregoing and other objects, aspects, and advantages will be better understood from the following detailed description of the invention with reference to the drawings, in which:

FIGS. 1 and 2 are diagrams showing a fault tolerant broadband network management system according to the invention.

FIG. 3 is a diagram showing connections between a broadband network management system and an ATM switch.

FIG. 4 is a diagram showing "manager" and "agent" software objects according to the invention.

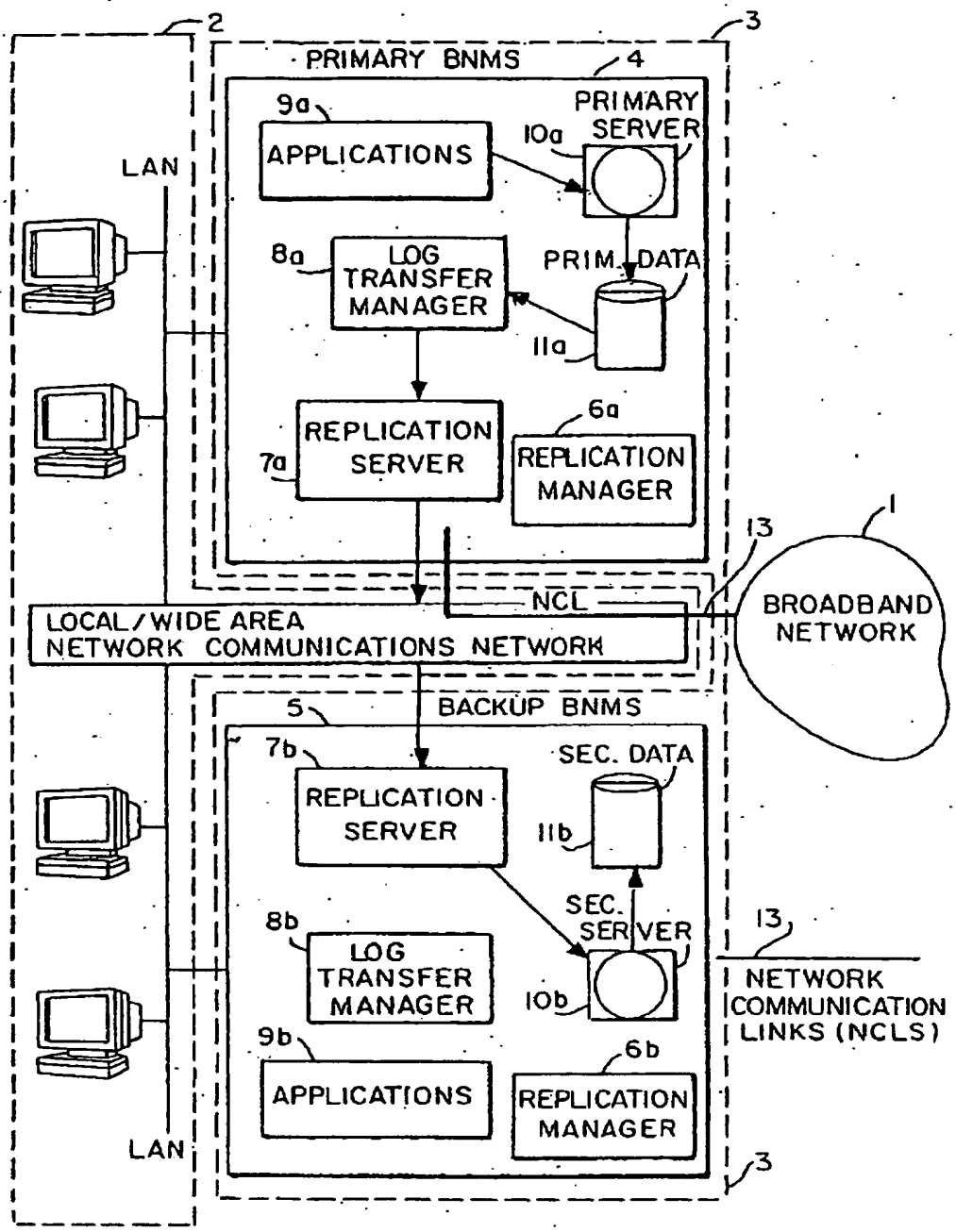
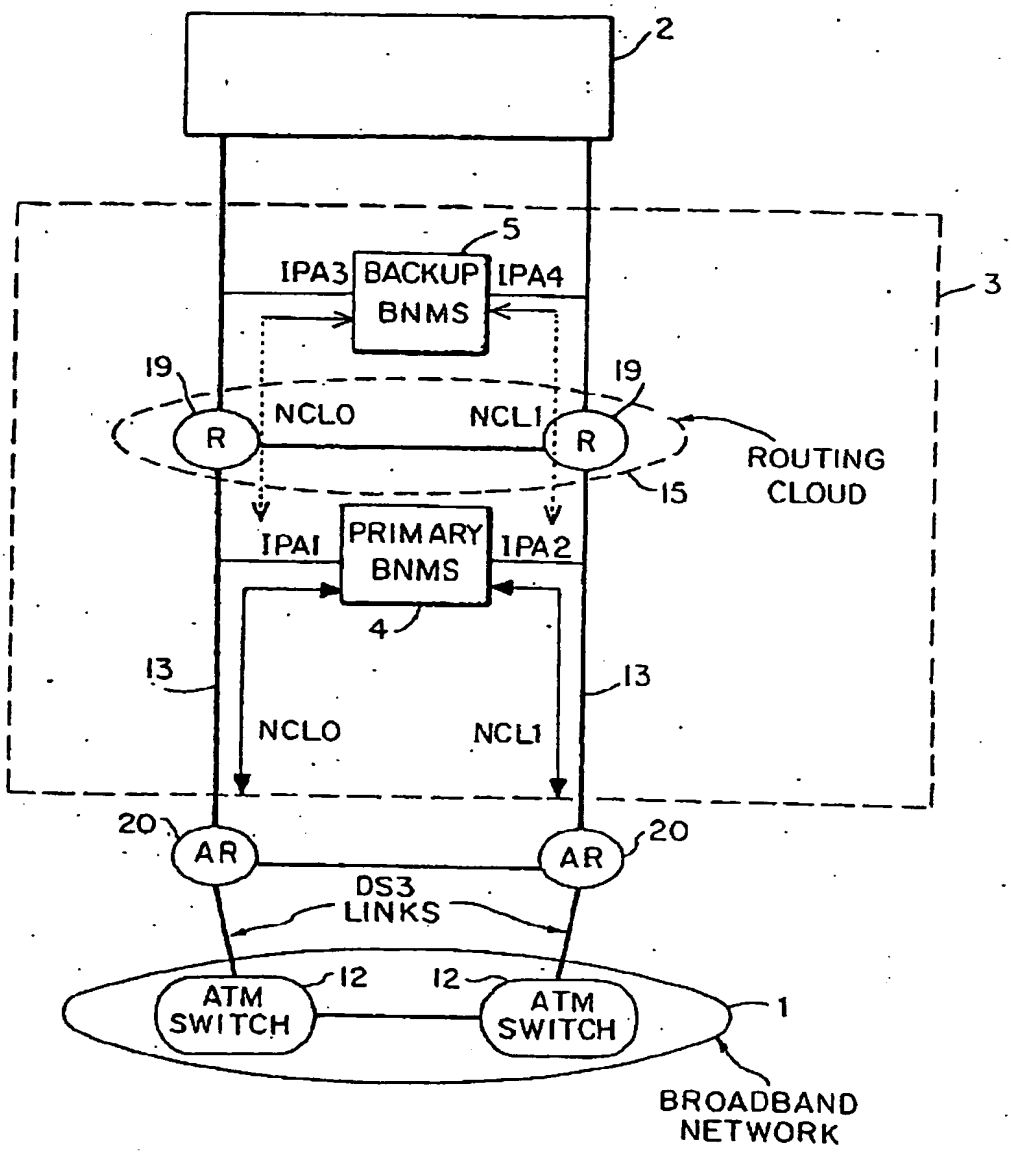

2
3
PRIMARY BNMS
4
9a
APPLICATIONS
PRIMARY SERVER
10a
LAN
8a
LOG TRANSFER MANAGER
PRIM. DATA
11a
REPLICATION SERVER
7a
6a
REPLICATION MANAGER
1
13
BROADBAND NETWORK
NCL
LOCAL/WIDE AREA NETWORK COMMUNICATIONS NETWORK
5
BACKUP BNMS
7b
REPLICATION SERVER
SEC. DATA
11b
SEC. SERVER
13
8b
LOG TRANSFER MANAGER
10b
NETWORK COMMUNICATION LINKS (NCLS)
9b
APPLICATIONS
6b
REPLICATION MANAGER
LAN
3

FIG. 1

FIG.2


2
5
IPA3
BACKUP BNMS
IPA4
3
19
19
NCL0
NCL1
R
R
ROUTING CLOUD
15
IPA1
PRIMARY BNMS
IPA2
4
13
13
NCL0
NCL1
20
AR
AR
20
DS3 LINKS
12
12
ATM SWITCH
ATM SWITCH
1
BROADBAND NETWORK

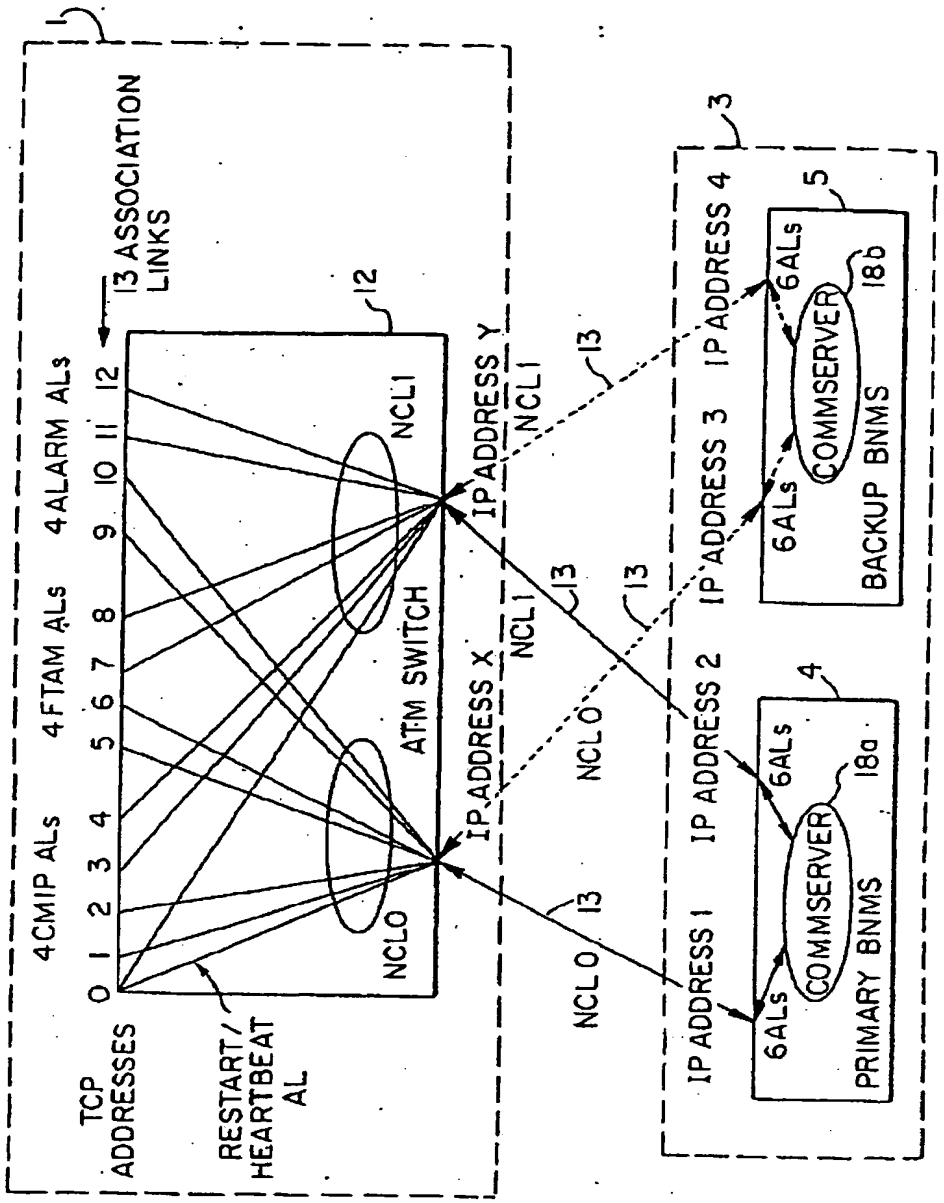

1
4CMIP ALs
4FTAM ALs
4ALARM ALs
13 ASSOCIATION LINKS
0 1 2 3 4 5 6 7 8 9 10 11 12
TCP ADDRESSES
RESTART/ HEARTBEAT AL
12
NCL0
NCL1
ATM SWITCH
IP ADDRESS X
IP ADDRESS Y
NCL0
NCL1
13
3
IP ADDRESS 1
IP ADDRESS 2
IP ADDRESS 3
IP ADDRESS 4
6ALs
COMMSERVER
PRIMARY BNMS
BACKUP BNMS
4
5
18a
18b

FIG.3

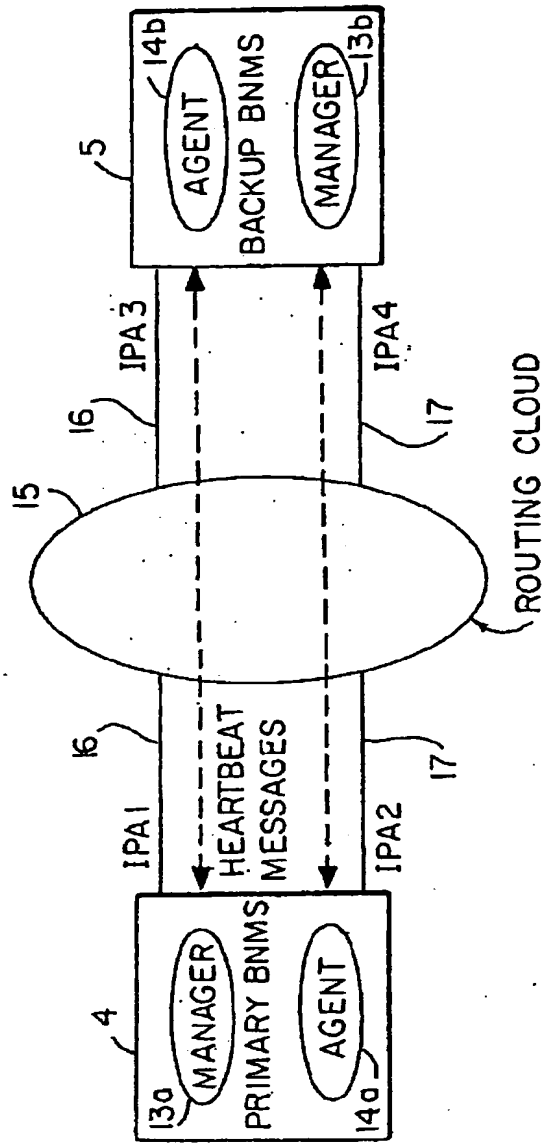

5
BACKUP BNMS
AGENT
14b
MANAGER
13b
IPA3
IPA4
16
17
15
ROUTING CLOUD
16
17
IPA1
HEARTBEAT MESSAGES
IPA2
4
PRIMARY BNMS
MANAGER
13a
AGENT
14a

FIG. 4

1. Abstract

ABSTRACT OF THE DISCLOSURE

A fault tolerant broadband network management system (BNMS) having primary and backup architecture used to effect automatic recovery in the event of a catastrophic failure. The database in the backup BNMS is kept synchronized with that of the primary BNMS via replication data servers in each BNMS. The architecture also uses a set of redundant Network Communication Links (NCLs) over which the BNMS communicates with the network elements. If there is a fault in the primary BNMS causing a failure of communication between the primary BNMS and the Broadband Network (BN), mechanisms are provided for the backup BNMS to take over the operation of monitoring and controlling the BN by switching over the NCLs from the primary BNMS to the backup BNMS automatically. When the backup BNMS takes over the management of the network, it assumes the primary BNMS role. When the original primary BNMS becomes operational again, it assumes the role of the backup BNMS, since the original backup BNMS has assumed the primary BNMS role. These roles as well as the NCLs can be switched for each occurrence of a fault.

2. Representative Drawing

Fig.1